

Secteur Tertiaire Informatique
Filière « Etude et développement »

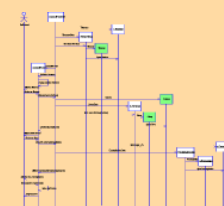
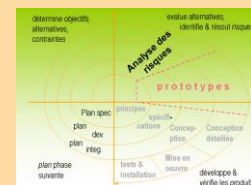
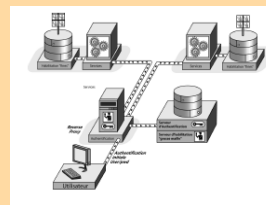
Séquence « Développer des pages web en lien
avec une base de données »

Prendre en compte le réseau dans la sécurité du
Web

Apprentissage

Mise en situation

Evaluation



Prendre en compte le réseau dans la sécurité du Web

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

| Version | Date | Auteur(s) | Action(s) |
|---------|----------|------------|----------------------|
| 1.0 | 20/07/16 | Lécu Régis | Création du document |

| | | |
|-------|--------------------------------------------------------------|----|
| 1. | Introduction | 6 |
| 2. | Sécuriser son réseau : objectifs | 6 |
| 2.1 | Connaître le système d'information | 6 |
| 2.1.1 | Identifier les composants du SI | 6 |
| 2.1.2 | Les types de réseau | 7 |
| 2.1.3 | Les interconnexions | 7 |
| 2.2 | Maîtriser le réseau | 8 |
| 2.2.1 | Sécuriser le réseau interne | 9 |
| 2.2.2 | BYOD « Bring Your Own Device » | 10 |
| 2.2.3 | Contrôler les échanges internes | 10 |
| 2.2.4 | Protéger le réseau interne d'internet | 10 |
| 2.2.5 | Accès distant | 11 |
| 2.2.6 | Sécuriser l'administration | 11 |
| 2.2.7 | Wifi | 12 |
| 3. | Sécuriser l'infrastructure réseau : les moyens | 12 |
| 3.1 | Pare-feu | 12 |
| 3.2 | Répartiteur de charges | 13 |
| 3.3 | IDS et IPS | 13 |
| 3.4 | VPN | 14 |
| 3.5 | Segmentation | 14 |
| 3.6 | Exemple pratique de sécurisation avec un réseau simple | 14 |
| 4. | La sécurité du protocole IP | 14 |
| 4.1 | Préambule | 14 |
| 4.2 | Exemple d'attaque par réflexion | 15 |
| 4.3 | Exemple d'écoute de trafic | 16 |
| 4.4 | Exemple de modification du routage des datagrammes IP | 16 |
| 4.5 | Sécurisation du protocole IP | 16 |
| 4.6 | Pour aller plus loin dans les protocoles IP et TCP | 16 |
| 5. | Ecoute du réseau avec WireShark | 17 |
| 5.1 | installation de WireShark | 17 |
| 5.2 | Démonstration de l'outil WireShark par le formateur | 17 |
| 5.3 | Mise en pratique | 17 |
| 6. | Conclusion | 17 |

Objectifs

A l'issue de cette séance, le stagiaire sera capable de :

- Identifier les principaux éléments d'une infrastructure réseau (Routeur, Commutateur, Pare-feu, Proxy) et comprendre leur rôle dans le réseau de l'entreprise
- Identifier les principaux protocoles réseau (IP, TCP, http, https) et leurs caractéristiques
- Faire le lien entre le réseau (infrastructure et protocole) et la sécurité de l'application Web en se posant des questions de base sur la sécurité :
 - dans le cas d'un Intranet, les informations sensibles sont-elles diffusées dans l'entreprise ?
 - les mots de passe circulent-ils en clair sur le réseau ?
 - dans le cas d'un site Web hébergé par l'entreprise, est-il séparé de l'informatique interne par une DMZ ?
 - y-a-t-il une possibilité d'attaque de type « *Man in the Middle* » entre le client et le serveur ?

Pré requis

Pas de pré requis technique en réseau.

La séance s'appuie sur le monde de l'entreprise. Il faut être utilisateur du réseau, si possible dans différents contextes (réseau local Ethernet, appareil nomade en 3G/4G, WIFI etc.) et être curieux techniquement.

Méthodologie

Ce document peut être utilisé en présentiel ou à distance.

Chaque slide du projet CyberEdu est accompagné d'un guide de lecture AFPA qui précise le vocabulaire technique, et propose des recherches complémentaires, avec des liens sur wikipedia.

Seule la mise en pratique optionnelle d'un analyseur de réseau (*sniffer*) requiert l'aide d'un formateur.

Mode d'emploi

Symboles utilisés :



Renvoie à des supports de cours, des livres ou à la documentation en ligne constructeur.



Propose des exercices ou des mises en situation pratiques.



Point important qui mérite d'être souligné !

Ressources

Documents du projet CyberEdu :

- [CyberEdu_module_2_hygiene_informatique.pdf](#)
(1 Connaître le système d'information, 2 Maîtriser le réseau)
- [CyberEdu_module_3_reseau_et_applicatifs.pdf](#)
(1 La sécurité du protocole IP, 2 Sécurisation du réseau)

Pour approfondir : [Deperimetrisation.pdf](#)

Article libre de droit sur une tendance actuelle en sécurité réseau

Document formateur : [CyberEdu_reseau.pdf](#)

La première fiche (capture du mot de passe avec *WireShark*) pourra donner lieu à une démonstration par le formateur et à une mise en pratique.

1. INTRODUCTION

L'objectif de cette séance n'est évidemment pas de s'improviser technicien ou ingénieur réseau.

Mais, dans le cadre de son métier, un développeur qui travaille dans une architecture client/serveur, web ou 4 tiers ne peut faire abstraction du réseau, sans exposer son application à de gros risques de sécurité : capture du mot de passe par écoute du réseau etc.

Une connaissance minimale de l'infrastructure de l'entreprise, de son réseau physique et des protocoles utilisés permettra de faire des choix de sécurité avec bon sens.

Cette culture technique sera utile dans plusieurs situations professionnelles, durant le cycle de développement du projet :

- **l'analyse** doit intégrer les risques réseau dans l'identification des besoins de sécurité de l'application Web : une application Intranet sur un réseau protégé réservé à des utilisateurs de confiance, demandera moins de sécurisation qu'un site Web ouvert au public ;
- **la conception** doit répondre aux besoins de sécurité identifiés dans l'analyse : chiffrer les mots de passe ;
- **le déploiement et l'accès à l'application** supposent certains choix réseau : protéger l'accès à une application critique par le protocole *https*.

Comme plusieurs des séances liées à la sécurité, cette séance va donner les repères minimaux sur les infrastructures et les protocoles, mais elle fournira aussi des références bibliographiques, pour approfondir le domaine.

Elle s'appuie sur les documents du projet CyberEdu, en proposant un parcours guidé :

- si vous êtes en formation présentielle, ces documents seront présentés par le formateur, qui répondra à vos questions ;
- vous pouvez aussi travailler de façon autonome en suivant les guides de lecture et en faisant des recherches complémentaires sur Internet.

2. SECURISER SON RESEAU : OBJECTIFS

Ouvrez le document CyberEdu : [CyberEdu_module_2_hygiene_informatique.pdf](#)

Si vous découvrez ce chapitre en autonomie, suivre ce



Guide de lecture

2.1 CONNAITRE LE SYSTEME D'INFORMATION

2.1.1 Identifier les composants du SI

(p. 5) La sécurisation du code est essentielle dans une démarche sécurité, puisque toute vulnérabilité logicielle aura des conséquences à plus haut niveau : application, système d'exploitation, voire SI (système d'information de l'entreprise).

Mais à l'inverse, un développement sécurisé n'est possible que si l'on prend en compte le SI de l'entreprise et son infrastructure réseau, qui auront des conséquences directes sur la manière de déployer notre application, les risques encourus et les attaquants possibles.

Le développement sécurisé ne peut se faire avec des œillères : il exige une ouverture d'esprit sur l'entreprise et le métier du client, qui peut partir d'un inventaire des biens et des métiers de l'entreprise, avec les risques encourus par chacun d'entre eux.

Prendre en compte le réseau dans la sécurité du Web

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

(p. 6) Rappelle le lien entre les actifs primordiaux (biens immatériels indispensables à la survie de l'entreprise), et les éléments support (applications, systèmes d'exploitation) qui les prennent en charge¹.

L'inventaire permet au développeur de prendre conscience des conséquences possibles d'une vulnérabilité dans son application : une attaque conduite à partir de cette application peut-elle s'étendre au SI ? Quels sont les actifs primordiaux qui pourraient être touchés par cette attaque (brevets, procédés de fabrication, image de l'entreprise) ?

La connaissance d'un SI commence par le référencement de ses équipements qui sont de deux types :

- les équipements internes à l'entreprise, référencés de façon unique par leur adresse MAC (adresse physique stockée dans la carte réseau) sont relativement faciles à gérer.



Sur la notion d'adresse MAC : https://fr.wikipedia.org/wiki/Adresse_MAC

- les équipements nomades n'ont pas d'adresse MAC et sont référencés par leur code IMEI (*International Mobile Equipment Identity*, numéro de série unique composé de 15 à 17 chiffres). Ces équipements sont souvent difficiles à gérer et à sécuriser.

L'entreprise subit actuellement une « déperimétrisation » due aux téléphones mobiles et tablettes que les salariés utilisent aussi dans l'entreprise. Le périmètre à défendre devient flou : un matériel mal protégé et utilisé dans un environnement domestique peut ensuite être connecté au SI de l'entreprise et vu comme un équipement interne ; il peut évidemment amener avec lui des virus et de nombreuses autres menaces.



Sur la notion de déperimétrisation, voir l'article [Deperimétrisation.pdf](#)

Questions pour le développeur :

- mon application est-elle destinée à un déploiement en local, dans un environnement sécurisé ?
- ou au contraire à des appareils nomades qui seront utilisés dans plusieurs contextes, professionnel et domestique, sécurisé et non sécurisé ?

2.1.2 Les types de réseau

(p. 6) Les plus connus :

- **LAN** (*Local Area Network*) : par exemple, notre réseau local ETHERNET à l'AFPA
- **WAN** (*Wide Area NetWork*) : Internet

Mais d'autres réseaux à des échelles intermédiaires, se sont développés avec les appareils nomades et sont autant de vecteurs d'attaque possibles :

PAN (*Personal Area NetWork*) et **WPAN** (*Wireless Pan*) : réseau informatique restreint en terme d'équipements, généralement mis en œuvre dans un espace d'une dizaine de mètres, et basé sur de l'USB, du Bluetooth, de l'infrarouge (IR), ou du [zigbee](#).

2.1.3 Les interconnexions

(p. 9) Le cauchemar de l'ingénieur réseau et sécurité :

¹ Vu dans la séance « Sensibiliser à la sécurité informatique »

- dans une entreprise désormais difficile à délimiter (la « déperimétrisation »), les équipements nomades circulent entre un environnement domestique non sécurisé et l'entreprise ;
- les types de réseau se sont multipliés ainsi que leurs modes d'interconnexion, ce qui accroît encore les vulnérabilités. Donnons deux exemples :

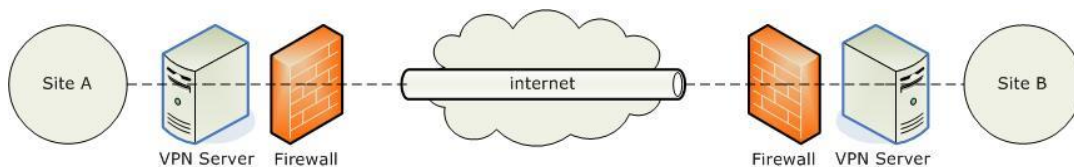
(1) USB

Recharger son mobile sur le port USB d'un PC de l'entreprise est une pratique courante, qui peut sembler anodine. Mais c'est aussi une interconnexion possible, via le port USB, entre un appareil nomade relié à Internet par une liaison 3G/4G non sécurisée, et le réseau interne de l'entreprise.

Cette interconnexion sauvage ne respecte pas le périmètre de l'entreprise et échappe à toutes ses règles de sécurisation : les flux échangés ne passent pas par le Pare-feu chargé d'isoler le réseau interne d'Internet.

(2) VPN

Le VPN (*Virtual Private Network*), réseau privé virtuel, est un système qui crée un lien direct entre des ordinateurs distants (dans les sites A et B).



La connexion entre les ordinateurs est gérée de façon transparente par le logiciel de VPN, créant un tunnel entre eux. Les ordinateurs connectés au VPN sont ainsi sur le même réseau local (virtuel), ce qui permet de passer outre aux restrictions sur le réseau (pare-feu, *Firewall*).

C'est une technique utile : elle permet de travailler à domicile, en accédant au réseau interne de l'entreprise et à ses serveurs, comme si l'on était sur place. Les informations échangées dans le tunnel du VPN sont chiffrées, pour échapper à une attaque venant d'Internet.

Mais le VPN peut aussi être un vecteur d'attaque :

Si l'on reprend le premier exemple, un mobile infecté par une application malveillante pourra ouvrir un VPN pour communiquer avec un serveur de *hack*, par une liaison 3G/4G.

Une fois le mobile connecté par le port USB au SI de l'entreprise, l'application malveillante pourra utiliser ce VPN pour recopier des données confidentielles de l'entreprise vers le serveur de *hack*.

2.2 MAITRISER LE RESEAU

De quels moyens l'ingénieur réseau et sécurité dispose-t-il pour gérer cette complexité et réduire les possibilités d'attaque ?

En tant que développeurs, nous ne mettrons pas en œuvre ces techniques, mais il faut les comprendre pour évaluer les risques qui pèseront sur notre application, lorsqu'elle sera déployée dans l'entreprise.

Ce document CyberEdu présente globalement les principaux dangers et les bonnes pratiques de sécurisation du réseau.

Nous reviendrons ensuite sur l'infrastructure réseau et les protocoles, et leur influence sur la sécurité de l'entreprise.

2.2.1 Sécuriser le réseau interne

(p.11) « Diviser pour mieux régner » : en partitionnant le réseau de l'entreprise, on limite les d'attaques et leur propagation. Cette division peut être physique ou logique :

Physique

Chaque bâtiment ou étage est équipé d'un réseau Ethernet distinct. Ces réseaux ne peuvent communiquer entre eux que par un **Routeur**, équipement réseau chargé d'acheminer et filtrer les messages entre plusieurs réseaux.



Sur la notion de Routeur : <https://fr.wikipedia.org/wiki/Routeur>

Logique

- Les sous-réseaux partagent le même support physique (par exemple, le même réseau Ethernet) mais sont séparés logiquement par leur adressage IP ;
- Les **VLAN** (*Virtual Local Network*) sont des réseaux logiques indépendants, gérés par un **Commutateur** (*Switch*).



Sur la notion de VLAN : https://fr.wikipedia.org/wiki/R%C3%A9seau_local_virtuel

Dans les trois cas, il est possible d'interdire à un utilisateur de sortir de son réseau, ou de filtrer ses échanges avec les autres parties de l'entreprise.

L'ingénieur réseau et sécurité applique les mêmes principes qu'en développement sécurisé : « Adopter une posture de méfiance » et « Séparer et minimiser les droits et les privilèges » :

- les utilisateurs de passage avec des équipements nomades, réputés peu sûrs, ne pourront avoir accès au WIFI et à Internet que dans une zone « visiteur ». Ils ne verront pas les stations de travail et les serveurs internes de l'entreprise ;
- l'utilisateur de base de l'entreprise aura accès à sa station de travail dans une zone « bureau », où il pourra se connecter à Internet en passant par un Pare-feu, et à certains serveurs de l'entreprise, selon ses droits ;
- l'administration des serveurs ne pourra se faire qu'à partir de la zone « serveur », pour les utilisateurs autorisés de l'équipe système.

On retrouve le modèle de *l'architecture militaire*, vu dans les premières séances sur le développement sécurisé : des secteurs retranchés qui ne peuvent communiquer que par des interfaces bien délimitées (*Pont-levis, herse, poterne pour le château-fort*, Routeur et Pare-feu pour le réseau).

La posture de méfiance exige de contrôler tous les accès et d'authentifier tous les utilisateurs par :

- un **certificat numérique**, qui peut être vu comme une carte d'identité numérique attestant de l'identité de l'utilisateur. Il est délivré par un organisme spécialisé et agréé, le tiers de confiance. Cette notion sera détaillée dans la séance suivante sur la cryptographie ;

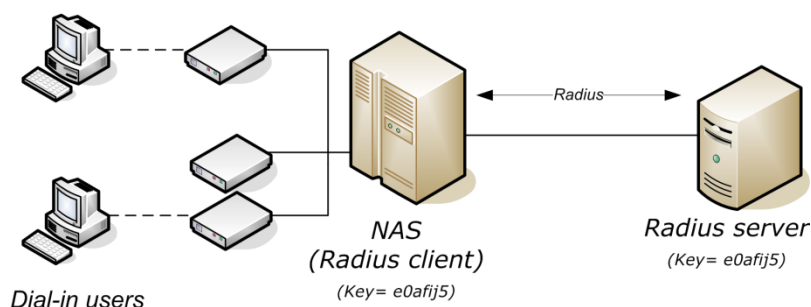


Sur la notion de certificat : https://fr.wikipedia.org/wiki/Certificat_%C3%A9lectronique

- une **carte à puce**, avec un identifiant unique (comme la carte SIM de votre mobile) ;
- un **serveur d'authentification**, type *RADIUS* : authentification centralisée de tous les utilisateurs, qui leur autorise certains réseaux ou sous-réseaux de l'entreprise, selon leur profil.

Prendre en compte le réseau dans la sécurité du Web

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »



2.2.2 BYOD « Bring Your Own Device »

(p. 12) La sécurisation d'un réseau suit donc une logique de retranchement et de sectorisation, dans le périmètre de l'entreprise.

Autoriser l'utilisateur à apporter son propre équipement dans l'entreprise, que ce soit un appareil mobile ou un PC portable, remet en cause ce périmètre, le rend perméable aux attaques issues de l'informatique domestique.

La défense périmétrique de l'entreprise sera alors insuffisante.

2.2.3 Contrôler les échanges internes

(p. 13) Autre formulation de la posture de méfiance, pour le contrôle des flux réseaux : « *Tout ce qui n'est pas explicitement autorisé est interdit* ».

Contrôler les échanges internes revient à bâtir une défense en profondeur : puisque le périmètre de l'entreprise devient perméable à cause des mobiles et des équipements BYOD, un contrôle externe, périmétrique, ne suffit plus ; il faut étendre les contrôles à tous les échanges de données internes à l'entreprise.

Comme les couches logicielles en développement sécurisé, chaque secteur de l'entreprise va revérifier l'identité de l'émetteur et ses autorisations, avant d'accepter ses données.

Les filtrages décrits doivent être effectués par un Pare-feu (*FireWall*).

Le Pare-feu permet de définir des règles (autorisation ou interdiction) pour tout flux réseau.

Il identifie l'émetteur et le destinataire du flux par son adresse et son port IP :

- l'adresse IP identifie une machine de façon unique (comme l'adresse postale d'un immeuble) ;
- mais de nombreux logiciels peuvent cohabiter et utiliser le réseau sur une même machine : pour identifier précisément un logiciel, le protocole IP lui associe une boîte aux lettres réseau (le « port » IP, équivalent de la boîte aux lettres d'un appartement dans l'immeuble).

Comme en développement sécurisé, il est préférable de raisonner positivement en utilisant des listes blanches des adresses IP autorisées, plutôt que de procéder par exclusion avec des listes noires.

2.2.4 Protéger le réseau interne d'internet

(p. 14) Cette tâche est également celle du Pare-feu : on fixera des règles plus strictes sur la branche du Pare-feu reliée à Internet, considéré bien entendu comme n'étant pas de confiance.

On retrouve la comparaison avec l'architecture militaire :

- la **DMZ** (zone démilitarisée) est une zone tampon entre la zone sûre du réseau interne et la zone non sûre d'Internet ;

Prendre en compte le réseau dans la sécurité du Web

- elle contient entre autres les serveurs Web hébergés par l'entreprise, qui doivent être accessibles de l'extérieur et sont donc susceptibles d'être attaqués et compromis.



Sur la notion de DMZ : [https://en.wikipedia.org/wiki/DMZ_\(computing\)](https://en.wikipedia.org/wiki/DMZ_(computing))

Un **IDS** (*Intrusion Detection System*, système de détection d'intrusion) est une « sonde » qui repère les activités anormales ou suspectes sur la cible analysée (réseau ou serveur). Il fait l'historique de toutes les tentatives d'intrusion, réussies ou en échec.



Sur la notion d'IDS :

https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_d%C3%A9tection_d%27intrusion

2.2.5 Accès distant

(p. 15) Avant les appareils nomade et le BYOD, c'était le cas d'utilisation le plus risqué : la demande vient de l'extérieur de l'entreprise (pour le château, au-delà du premier rempart) et justifie d'adopter une posture de méfiance maximum.

Il est plus facile à traiter que le BYOD car il ne remet pas en cause le périmètre de l'entreprise et le concept de défense périmétrique. Mais il peut exiger plusieurs outils qui jouent des rôles différents dans la défense :

- le serveur d'authentification (*RADIUS*) garantit l'identité du demandeur : on ne parle pas à un inconnu ;
- le VPN garantit la confidentialité de l'échange et la non interception des informations de sécurité en traversant Internet, par une attaque de type *Man in the Middle*. Sans le VPN, le serveur d'authentification n'est sûr qu'au premier échange ! Dans les échanges suivants, il reconnaît soit le vrai utilisateur, soit un usurpateur qui a intercepté la première connexion.



Principe de l'attaque : https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu

(p. 16) Dans la même logique, il faut également chiffrer les échanges après l'étape de connexion, pour éviter le piratage de données confidentielles.

- **telnet** est une commande en mode texte, qui permet de se connecter à distance et d'envoyer des commandes à des serveurs UNIX ou Windows. Mais elle n'est pas chiffrée : tout l'échange passe en clair sur le réseau ;
- il faut donc lui préférer la commande **ssh** qui chiffre les données transmises ;
- pour une application web, on utilisera le protocole sécurisé **https** de préférence à **http** qui transmet les données en clair ;
- il existe des variantes sécurisées de toutes les commandes : par exemple **sftp** pour échanger des fichiers sur le réseau, à la place de la commande **ftp** qui émet en clair.

2.2.6 Sécuriser l'administration

(p. 17) Les bons choix sont déductibles de ce qui précède :

- en vertu du principe de « *séparation et minimisation des privilèges* », et de la « *posture de méfiance* », on ne confiera pas le plus important (l'administration du réseau et des serveurs) au moins sûr (une interface d'administration depuis Internet) ;

Prendre en compte le réseau dans la sécurité du Web

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

- comme le réseau d'entreprise dans son ensemble ne peut lui-même être considéré comme totalement sûr, on construira un « réseau dans le réseau », mieux sécurisé et réservé à l'administration système et réseau (**le donjon, isolé du premier rempart**).

2.2.7 Wifi

(pp. 18-19)

Conseils techniques de sécurisation pour le Wifi : à lire et mettre en pratique chez vous.

(p. 20) :

Bonnes pratiques pour l'utilisation d'un Wifi public : à recommander.

3. SECURISER L'INFRASTRUCTURE RESEAU : LES MOYENS

Le chapitre précédent a décrit les objectifs d'un ingénieur réseau et sécurité, en charge de la sécurisation d'un réseau.

Nous avons vu que les principes de sécurisation étaient les mêmes qu'en développement :

- adopter une posture de méfiance
- séparer et minimiser les droits et les privilèges
- pratiquer une défense périmétrique (en l'absence d'informatique nomade et de BYOD)
- compléter la défense périmétrique par une défense en profondeur dans les autres cas.

Pour les lecteurs qui n'ont pas de culture technique réseau, nous avons donné quelques indications au fil de l'eau et des liens vers wikipedia pour approfondir.

Nous allons maintenant préciser le rôle des principaux équipements dans la sécurisation d'un réseau, à partir des slides de CyberEdu et de wikipedia.

Ouvrez le document CyberEdu :

[CyberEdu_module_3_reseau_et_applicatifs.pdf](#), chap.2 « Sécurisation d'un réseau »

Si vous découvrez ce chapitre en autonomie, suivre ce



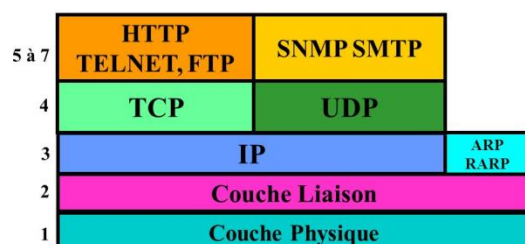
Guide de lecture

3.1 Pare-feu

(p. 12-13)

https://fr.wikipedia.org/wiki/Pare-feu_%28informatique%29

Un protocole réseau définit les formats des données échangées (*trames, paquets*), et la dynamique des échanges.



Les protocoles sont hiérarchisés et forment une pile (ci-dessus), dans laquelle un protocole de couche N ne peut appeler que la couche N-1.

Prendre en compte le réseau dans la sécurité du Web

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

Parmi les protocoles les plus connus :

- **IP** gère la couche 3 : **Réseau**.

Il prend en charge la transmission des paquets dans le réseau TCP/IP.

https://fr.wikipedia.org/wiki/Internet_Protocol

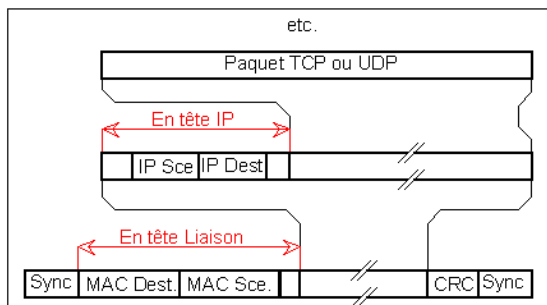
- **TCP** gère la couche 4 : **Transport**.

Il établit une connexion entre l'émetteur et le destinataire.

Une connexion TCP est comparable à une communication téléphonique.

A chaque envoi d'un message, TCP appelle la couche IP qui va ranger le paquet TCP dans sa partie donnée, en lui ajoutant une entête IP contenant les adresses expéditeur et destinataire.

On parle comme en objet, « d'encapsulation » de trames :



[https://fr.wikipedia.org/wiki/Encapsulation_\(r%C3%A9seau\)](https://fr.wikipedia.org/wiki/Encapsulation_(r%C3%A9seau))

- **UDP** occupe la même couche que TCP, mais travaille en mode déconnecté : il envoie chaque message (*datagramme*) sans garantir sa chronologie (comme un envoi de courrier).

Un Pare-feu gère à la fois les protocoles bas niveau TCP, UDP et IP, chargés du transfert des informations, et les protocoles applicatifs comme HTTP, DNS et SMTP qui interprètent les données transmises :

- **DNS** (*Domain Name System*) : protocole qui permet entre autres, de retrouver l'adresse IP d'un site à partir de son URL ;
- **SMTP** : (*Simple Mail Transfer Protocol*) : protocole utilisé par les serveurs de messagerie.

3.2 Répartiteur de charges

(p. 14)

Nous avons vu que certaines vulnérabilités dans les applications, par exemple des requêtes SQL très lentes pour certains jeux de données, facilitent les attaques par déni de service.

Mais aucune précaution applicative n'est suffisante pour les éviter, surtout pour les attaques massives conduites à partir d'un *botnet*.

L'utilisation d'un répartiteur de charge augmente la résistance à ces attaques, sans parvenir à les éviter dans tous les cas : cela dépend de la taille du *botnet* utilisé.

3.3 IDS ET IPS

(p. 18-19)

https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_d%C3%A9tection_d%27intrusion

Prendre en compte le réseau dans la sécurité du Web

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

3.4 VPN

(p. 20-23)

https://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel

Quelle que soit la technologie du VPN, le but est d'éviter l'attaque du type *Man in the middle* : sans VPN, un espion placé entre l'émetteur et le récepteur parvient à lire les données qui transitent, voire à les corrompre.

3.5 SEGMENTATION

(p. 24-26)

Nous avons vu dans le premier chapitre, l'importance de la segmentation d'un réseau dans sa sécurisation. Les slides détaillent les différentes manières de segmenter.

(p. 25) Les réseaux complètement isolés ne relèvent pas de l'humour noir : ils sont rares, mais nécessaires dans des environnements militaires ou industriels critiques, qui doivent être complètement déconnectés d'Internet.

(p. 27) Un *trunk* est un lien physique permettant le transit entre plusieurs VLAN.

3.6 EXEMPLE PRATIQUE DE SECURISATION AVEC UN RESEAU SIMPLE

(p. 28-39)

Lire attentivement cette étude de cas qui met en pratique nos deux premiers chapitres sur la sécurisation du réseau.

(p. 28) Le cahier des charges soumis à l'ingénieur réseau et sécurité

(p. 29) L'existant : aucune sécurité

(p. 31) Un seul Pare-feu frontal : défense périmétrique qui sépare l'extérieur de l'intérieur de l'entreprise, mais ne tient pas compte des différents types d'utilisateur, qui ont tous les mêmes accès réseau.

(p. 32) Un exemple de défense en profondeur avec un deuxième pare-feu spécialisé dans le filtrage des flux internes à l'entreprise. Le pare-feu frontal continue à assurer la défense périmétrique.

4. LA SECURITE DU PROTOCOLE IP

Ouvrez le document CyberEdu :

[CyberEdu_module_3_reseau_et_applicatifs.pdf](#), chap.1 « La sécurité du protocole IP »

Si vous découvrez ce chapitre en autonomie, suivre ce



Guide de lecture

4.1 PREAMBULE

(p. 5)

Toutes ces remarques s'appliquent aussi malheureusement au protocole *http* qui :

- n'était conçu au départ que pour télécharger des pages web statiques ;

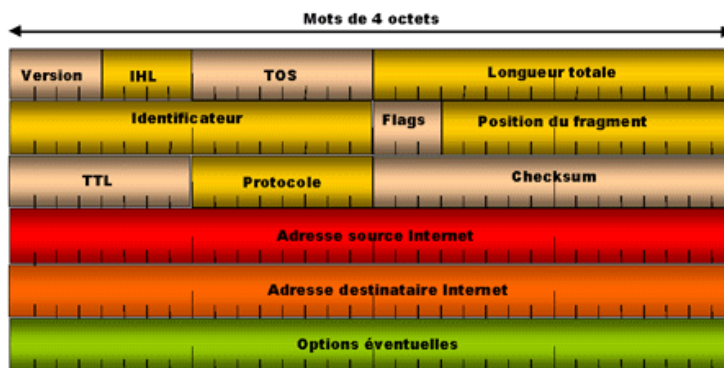
Prendre en compte le réseau dans la sécurité du Web

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

- sert aujourd'hui à toute autre chose : appeler des pages dynamiques *jsp*, *asp*, *php*, c'est-à-dire de véritables applications ;
- mais le protocole lui-même n'a pas été modifié (ou peu) et n'intègre pas les propriétés de sécurité nécessaires pour bien sécuriser ces applications web ;
- la sécurisation repose donc sur des surcouches (par exemple le chiffrement des données) et tient du pari : il faut revoir sa copie au fur et à mesure de la découverte de nouvelles vulnérabilités web (voir séance « Identifier les failles de sécurité et appliquer les bonnes pratiques de sécurisation des applications Web »).

Dans un *datagramme* IP, l'adresse source est renseignée par l'émetteur, sans contrôle :

- un navigateur ou une application sérieuse vont mettre la vraie adresse de l'émetteur ;
- mais un programme C malveillant peut ranger ce qu'il veut dans l'adresse source, en usurpant l'identité d'un autre utilisateur ;
- de la même manière, un routeur compromis peut changer l'adresse destinataire afin que le *datagramme* se perde, ou soit envoyé à un utilisateur malveillant.



4.2 EXEMPLE D'ATTAQUE PAR REFLEXION

La commande *ping* sert en réseau pour déterminer si un serveur est actif, pour vérifier son adresse IP ou son nom de serveur, pour vérifier le routage.

Elle envoie un message de service **ICMP** (*Internet Control Message Protocol*) au destinataire, qui en fait l'écho (ping-pong d'où le nom de la commande).



Sur ICMP : https://fr.wikipedia.org/wiki/Internet_Control_Message_Protocol

Essayez la commande *ping* (1 fois, sinon vous serez accusé par le destinataire de déni de service !)

```

C:\Users\regis.DEU>ping www.afpa.fr

Envoi d'une requête 'ping' sur www.afpa.fr [212.99.102.104] avec 32 octets de données :
Réponse de 212.99.102.104 : octets=32 temps=54 ms TTL=51
Réponse de 212.99.102.104 : octets=32 temps=52 ms TTL=51
Réponse de 212.99.102.104 : octets=32 temps=52 ms TTL=51
Réponse de 212.99.102.104 : octets=32 temps=53 ms TTL=51

Statistiques Ping pour 212.99.102.104:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 52ms, Maximum = 54ms, Moyenne = 52ms
  
```

L'attaque par réflexion consiste à placer une fausse adresse source (*adr_victime*) dans le datagramme IP, grâce à l'option **S** de la commande **ping** :

ping adr_destinataire -S adr_victime

Prendre en compte le réseau dans la sécurité du Web

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

4.3 EXEMPLE D'ECOUTE DE TRAFIC

C'est une méthode simple, proposée en mise en pratique optionnelle :

- elle utilise un espion réseau (*sniffer*) comme *WireShark* ;
- elle peut avoir des conséquences graves si l'on parvient à capturer les informations de sécurité, identifiants et mots de passe qui passent en clair sur le réseau.

Deux méthodes de sécurisation :

- sectorisation du réseau : pour réduire les possibilités d'écoute du réseau ;
- chiffrement des informations transmises : pour rendre les captures inexploitable.

4.4 EXEMPLE DE MODIFICATION DU ROUTAGE DES DATAGRAMMES IP

C'est une attaque un peu technique qui exige de connaître le modèle de routeur, et de casser son mot de passe administrateur.

Elle est facilitée par des routeurs mal configurés qui conservent leur mot de passe d'administration par défaut :



Liste des mots de passe par défaut, pour les différents constructeurs de routeur

<http://www.sosmotdepasse.com/mot-de-passe-par-defaut.html>

4.5 SECURISATION DU PROTOCOLE IP

Plusieurs méthodes de sécurisation :

1) La cryptographie

- Chiffrement des communications
- Authentification des entités

Les deux vont souvent ensemble : on veut savoir à qui l'on parle et ne pas être espionné.

2) La segmentation

- Cloisonnement du réseau
- Filtrage
- Dimensionnement adapté des infrastructures

3) La gestion technique du réseau

- Règles de renforcement de configuration des équipements
- Supervision etc.

4.6 POUR ALLER PLUS LOIN EN TCP/IP

Il existe de nombreux cours en ligne sur les réseaux et TCP/IP.

Dans les références sérieuses : formation gratuite à TCP/IP par un formateur CISCO :

<http://cisco.goffinet.org/introduction-a-tcp-ip#.V48jk6Kmpv0>

Ce site propose également des QUIZZ gratuits pour évaluer son niveau en réseau.

5. ECOUTE DU RESEAU AVEC WIRESHARK

Cette mise en pratique optionnelle n'est pas en autoformation : elle sera faite en présentiel, avec l'aide d'un formateur ayant des compétences réseau.

L'objectif est de mettre en évidence les risques de compromission (Confidentialité et Intégrité) des données qui transitent sur le réseau.

A l'aide d'un *sniffer* comme *WireShark*, on montre par exemple que les mots de passe transitent en clair dans des protocoles comme **ftp** et **http**.

5.1 INSTALLATION DE WIRESHARK

Téléchargez WireShark sur le site : <https://www.wireshark.org/>

Le site propose une formation en ligne *WireShark Training*, qui permet de prendre en main l'outil.

5.2 DEMONSTRATION DE WIRESHARK PAR LE FORMATEUR

On s'inspirera librement du scénario pédagogique donné dans le document :

[CyberEdu_reseau.pdf](#), Fiche 1 « Capture de données sur les réseaux »

5.3 MISE EN PRATIQUE

Elle doit se faire sous la responsabilité d'un formateur, pour d'éviter les débordements : capture de vrais mots de passe, stagiaire ou formateur !

6. CONCLUSION

En tant que développeur, nous n'interviendrons pas directement sur les méthodes de sécurisation liées au cloisonnement du réseau, au filtrage, à l'amélioration de la configuration des équipements.

Mais la compréhension de l'infrastructure réseau où sera déployée notre application, permettra de faire les bons choix de développement sécurisé :

- chiffrement applicatif des mots de passe et/ou des données, avant leur envoi sur le réseau ;
- utilisation de liaisons sécurisées dans les applications Web : *https*

(Voir séance « *Utiliser la cryptographie et les mécanismes de sécurité du Web* »)

CRÉDITS

OEUVRE COLLECTIVE DE L'AFPA

Sous le pilotage de la DIIP
et du centre sectoriel Tertiaire

EQUIPE DE CONCEPTION

Chantal PERRACHON – IF Neuilly-sur-Marne
Régis Lécu – Formateur AFPA Pont de Claix

Reproduction interdite

Article L 122-4 du code de la propriété intellectuelle.

« Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droits ou ayants cause est illicite. Il en est de même pour la traduction, l'adaptation ou la reproduction par un art ou un procédé quelconque. »

Prendre en compte le réseau dans la sécurité du Web

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »